

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-179627

(43)Date of publication of application : 27.06.2003

(51)Int.Cl.

H04L 12/56

G09C 1/00

H04L 9/36

H04L 12/22

(21)Application number : 2001-376217

(71)Applicant : MITSUBISHI ELECTRIC CORP

(22)Date of filing : 10.12.2001

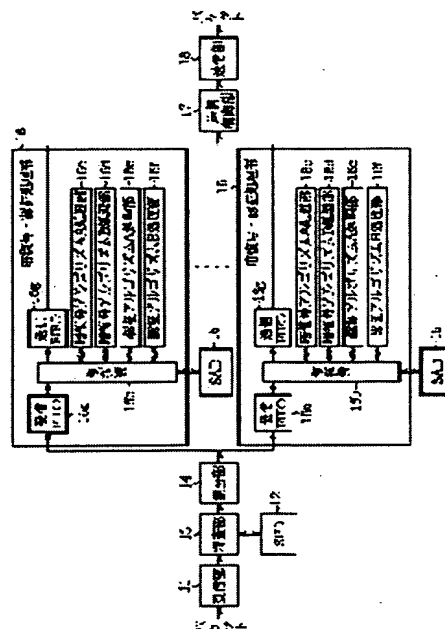
(72)Inventor : KONUKI JUNJI

(54) PACKET COMMUNICATION EQUIPMENT AND PACKET COMMUNICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To provide packet communication equipment capable of promptly starting execution of a cipher processing or the like, and a packet communication method.

SOLUTION: At the time of receiving a packet to which an index is added, a cipher algorithm and a key for ciphering, etc., are acquired from a specific entry specified by the index and the cipher processing or the like to the packet is executed.



LEGAL STATUS

[Date of request for examination]

15.11.2004

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-179627

(P2003-179627A)

(43) 公開日 平成15年6月27日 (2003.6.27)

(51) Int.Cl. ⁷	識別記号	F I	テマコード [*] (参考)
H 0 4 L 12/56		H 0 4 L 12/56	Z 5 J 1 0 4
G 0 9 C 1/00	6 6 0	G 0 9 C 1/00	6 6 0 E 5 K 0 3 0
H 0 4 L 9/36		H 0 4 L 12/22	
12/22		9/00	6 8 5

審査請求 未請求 請求項の数10 O L (全 10 頁)

(21) 出願番号 特願2001-376217(P2001-376217)

(22) 出願日 平成13年12月10日 (2001. 12. 10)

(71) 出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72) 発明者 小貫 淳史

東京都千代田区丸の内二丁目2番3号 三

菱電機株式会社内

(74) 代理人 100066474

弁理士 田澤 博昭 (外1名)

Fターム(参考) 5J104 AA18 DA04 EA16 JA31 NA01

PA07

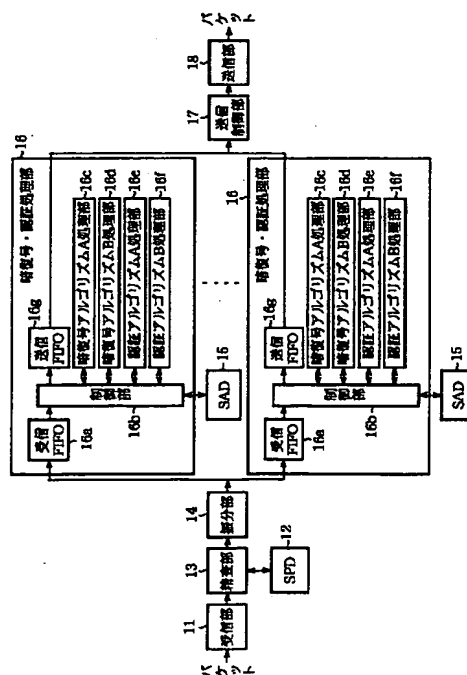
5K030 GA15 HA08 JA05 KA07 LD19

(54) 【発明の名称】 パケット通信装置及びパケット通信方法

(57) 【要約】

【課題】 振分部5がパケットを暗復号・認証処理部6に転送する際、暗号アルゴリズムや暗号鍵等をパケットに付加して転送する必要がある。このため、パケットの通信路の帯域が圧迫されて、そのパケットの転送に長時間を要し、暗復号・認証処理部6が速やかに暗号処理や認証処理の実行を開始することができない課題があった。

【解決手段】 インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵等を取得して、そのパケットに対する暗号処理等を実行する。



【特許請求の範囲】

【請求項1】 バケットを受信すると、そのバケットに係るデータベース内の特定エントリを指定するインデックスを当該バケットに付加するインデックス付加手段と、上記インデックス付加手段によりインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのバケットに対する暗号処理を実行する処理実行手段とを備えたバケット通信装置。

【請求項2】 バケットを受信すると、そのバケットに係るデータベース内の特定エントリを指定するインデックスを当該バケットに付加するインデックス付加手段と、上記インデックス付加手段によりインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのバケットに対する復号処理を実行する処理実行手段とを備えたバケット通信装置。

【請求項3】 バケットを受信すると、そのバケットに係るデータベース内の特定エントリを指定するインデックスを当該バケットに付加するインデックス付加手段と、上記インデックス付加手段によりインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのバケットに対する認証処理を実行する処理実行手段とを備えたバケット通信装置。

【請求項4】 複数の処理実行手段を設けて、インデックス付加手段が未処理中の処理実行手段に対してバケットを出力することを特徴とする請求項1から請求項3のうちのいずれか1項記載のバケット通信装置。

【請求項5】 各処理実行手段毎に同一のデータベースを設けたことを特徴とする請求項4記載のバケット通信装置。

【請求項6】 データベースに格納されている情報を変更するための特定バケットを受信すると、その特定バケットに格納されているデータにしたがって上記データベースを更新する更新手段を設けたことを特徴とする請求項1から請求項5のうちのいずれか1項記載のバケット通信装置。

【請求項7】 インデックス付加手段は、データベースに格納されている情報を変更するための特定バケットを受信すると、その特定バケットをバッファに一時的に保存し、処理実行手段は未処理のバケットが存在しないとき当該特定バケットを取得し、その特定バケットに格納されているデータにしたがって上記データベースを更新することを特徴とする請求項1から請求項5のうちのいずれか1項記載のバケット通信装置。

【請求項8】 バケットを受信すると、そのバケットに係るデータベース内の特定エントリを指定するインデックスを当該バケットに付加して出力する一方、そのインデックスが付加されたバケットを受けると、そのインデ

ックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのバケットに対する暗号処理を実行するバケット通信方法。

【請求項9】 バケットを受信すると、そのバケットに係るデータベース内の特定エントリを指定するインデックスを当該バケットに付加して出力する一方、そのインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのバケットに対する復号処理を実行するバケット通信方法。

【請求項10】 バケットを受信すると、そのバケットに係るデータベース内の特定エントリを指定するインデックスを当該バケットに付加して出力する一方、そのインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのバケットに対する認証処理を実行するバケット通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、バケットに対する暗号処理や認証処理を行うバケット通信装置及びバケット通信方法に関するものである。

【0002】

【従来の技術】近年のインターネットの普及に伴って、それらを利用した企業間のデータ通信が増えてきている。そのためデータの盗聴や改竄が大きな問題となっている。この問題を解決するには、暗号技術と認証技術が必須となる。通信装置間を接続する通信路上を流れるバケットを暗号化し、さらに認証コードを付加して送受信することにより、バケットの盗聴および改竄を防止することができる。

【0003】特に、最近では、処理するバケットの宛先アドレスやプロトコルに応じて暗号のアルゴリズムや認証のアルゴリズムを変更できる場合が多い。ここでは、そのような通信装置を考える。また、暗号処理や認証処理には膨大な計算量が必要であり、そのため通信装置内に暗号処理や認証処理を実行するバケット処理系を複数配置して、それらの間で並列処理を行う方式を用いる場合が多い。

【0004】図7は従来のバケット通信装置を示す構成図であり、図において、1は外部装置からバケットを受信する受信部、2は各バケットの宛先アドレスやセキュリティアソシエーションデータベース（以下、SADという）4内の特定エントリを指定するインデックス等を格納するセキュリティポリシーデータベース（以下、SPDという）、3は受信部1により受信されたバケットからIPヘッダを取り出し、そのIPヘッダ内の宛先アドレスをキーにして、SPD2から当該バケットに係るSAD4内の特定エントリを指定するインデックス（特定エントリのアドレスを示すポインタ）を取得する精査

部である。

【0005】4はバケットに対する暗号アルゴリズムや暗号用鍵等から構成されるエントリを複数個格納するSAD、5は精査部3により取得されたインデックスが指定するSAD4内の特定エントリから暗号アルゴリズムや暗号用鍵等を取得して、これらの暗号アルゴリズム等を当該バケットに付加し、そのバケットを未処理中の暗復号・認証処理部6に転送する振分部、6は振分部5により転送されたバケットから暗号アルゴリズム等を取り出して、そのバケットに対する暗号処理や認証処理を実行する暗復号・認証処理部、7は各暗復号・認証処理部6による処理後のバケットの順序を整列して、受信部1により受信されたバケットの順序に合わせる送信制御部、8は送信制御部7から出力されたバケットを送信する送信部である。

【0006】次に動作について説明する。受信部1が例えば平文データが格納されているバケットを受信すると、精査部3は、受信部1により受信されたバケットからIPヘッダを取り出し、そのIPヘッダからバケットの宛先アドレスを取得する。そして、精査部3は、その宛先アドレスをキーにして、SPD2から当該バケットに係るSAD4内の特定エントリを指定するインデックス（特定エントリのアドレスを示すポインタ）を取得する。

【0007】振分部5は、精査部3がSAD4内の特定エントリを指定するインデックスを取得すると、そのインデックスが指定するSAD4内の特定エントリから暗号アルゴリズム、認証アルゴリズム、暗号用鍵及び認証用鍵を取得する。そして、振分部5は、特定エントリから取得した暗号アルゴリズム等を当該バケットに付加し、そのバケットを未処理中の暗復号・認証処理部6に転送する。

【0008】暗復号・認証処理部6は、振分部5からバケットを受けると、そのバケットから暗号アルゴリズム等を取り出し、そのバケットに対する暗号処理や認証処理を実行する。送信制御部7は、各暗復号・認証処理部6から処理後のバケットを受けると、処理後のバケットの順序を整列して、受信部1により受信されたバケットの順序に合わせるようにする。送信部8は、送信制御部7から出力されたバケットを外部装置に送信する。

【0009】

【発明が解決しようとする課題】従来のバケット通信装置は以上のように構成されているので、振分部5がバケットを暗復号・認証処理部6に転送する際、暗号アルゴリズムや暗号鍵等をバケットに付加して転送する必要がある。このため、バケットの通信路の帯域が圧迫されて、そのバケットの転送に長時間を要し、暗復号・認証処理部6が速やかに暗号処理や認証処理の実行を開始することができない課題があった。

【0010】この発明は上記のような課題を解決するた

めになされたもので、速やかに暗号処理等の実行を開始することができるバケット通信装置及びバケット通信方法を得ることを目的とする。

【0011】

【課題を解決するための手段】この発明に係るバケット通信装置は、インデックス付加手段によりインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのバケットに対する暗号処理を実行する処理実行手段を設けたものである。

【0012】この発明に係るバケット通信装置は、インデックス付加手段によりインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのバケットに対する復号処理を実行する処理実行手段を設けたものである。

【0013】この発明に係るバケット通信装置は、インデックス付加手段によりインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのバケットに対する認証処理を実行する処理実行手段を設けたものである。

【0014】この発明に係るバケット通信装置は、複数の処理実行手段を設けて、インデックス付加手段が未処理中の処理実行手段に対してバケットを出力するようにしたものである。

【0015】この発明に係るバケット通信装置は、各処理実行手段毎に同一のデータベースを設けたものである。

【0016】この発明に係るバケット通信装置は、データベースに格納されている情報を変更するための特定バケットを受信すると、その特定バケットに格納されているデータにしたがってデータベースを更新する更新手段を設けたものである。

【0017】この発明に係るバケット通信装置は、インデックス付加手段がデータベースに格納されている情報を変更するための特定バケットを受信すると、その特定バケットをバッファに一時的に保存し、処理実行手段が未処理のバケットが存在しないとき特定バケットを取得し、その特定バケットに格納されているデータにしたがってデータベースを更新するようにしたものである。

【0018】この発明に係るバケット通信方法は、インデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのバケットに対する暗号処理を実行するようにしたものである。

【0019】この発明に係るバケット通信方法は、インデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのバケットに対する復号処理を

実行するようにしたものである。

【0020】この発明に係るバケット通信方法は、インデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのバケットに対する認証処理を実行するようにしたものである。

【0021】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態1. 図1はこの発明の実施の形態1によるバケット通信装置を示す構成図であり、図において、11は外部装置からバケットを受信する受信部、12は各バケットの送信先アドレスやSAD15内の特定エントリを指定するインデックス等を格納するSPD、13は受信部11により受信されたバケットからIPヘッダを取り出し、そのIPヘッダ内の送信先アドレス等をキーにして、SPD12から当該バケットに係るSAD15内の特定エントリを指定するインデックス（特定エントリのアドレスを示すポインタ）を取得し、そのインデックスを当該バケットに付加する精査部、14は精査部13によりインデックスが付加されたバケットを未処理中の暗復号・認証処理部16に転送する振分部である。なお、受信部11、SPD12、精査部13及び振分部14からインデックス付加手段が構成されている。

【0022】15はバケットに対する暗号アルゴリズムや暗号用鍵等から構成されるエントリを複数個格納するSAD（データベース）、16は振分部14からバケットを受けると、そのバケットに付加されているインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵等を取り出して、そのバケットに対する暗号処理や認証処理を実行する暗復号・認証処理部（処理実行手段）、16aは振分部14から転送されたバケットを受信して格納する受信FIFO、16bは受信FIFO16aに格納されているバケットを取得して、そのバケットに付加されているインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵等を取り出し、各種処理部を制御する制御部、16cは暗号アルゴリズムAを実行する暗復号アルゴリズムA処理部、16dは暗号アルゴリズムBを実行する暗復号アルゴリズムB処理部、16eは認証アルゴリズムAを実行する認証アルゴリズムA処理部、16fは認証アルゴリズムBを実行する認証アルゴリズムB処理部、16gは処理後のバケットを格納する送信FIFOである。

【0023】17は各暗復号・認証処理部16による処理後のバケットの順序を整列して、受信部11により受信されたバケットの順序に合わせる送信制御部、18は送信制御部17から出力されたバケットを送信する送信部である。なお、図3及び図4はこの発明の実施の形態1によるバケット通信方法を示すフローチャートである。

【0024】次に動作について説明する。最初に平文データが格納されているバケットを暗号化して、そのバケットに認証コード（認証用のダイジェスト）を付加する場合について説明する。受信部11が外部装置から平文データが格納されているバケットを受信すると、そのバケットのMACヘッダを削除して精査部13に出力する（ステップST1）。

【0025】精査部13は、受信部11からバケットを受けると、そのバケットからIPヘッダを取り出し、そのIPヘッダからバケットの送信元アドレス、送信先アドレスやプロトコル等を取得する。そして、精査部13は、そのアドレスやプロトコルと一致するSPD12内のエントリを検索する（ステップST2）。

【0026】即ち、SPD12は、図2に示すように、送信元アドレス、送信先アドレス、プロトコル、送信先ポート番号、送信元ポート番号、SPI、処理指定（バケットに対する処理内容）、及びインデックス（SAD15内の特定エントリのアドレスを示すポインタ）から構成された複数個のエントリを格納しているので、IPヘッダから取得したアドレスやプロトコルと一致する内容を有するエントリを検索する。ただし、必要に応じて送信先アドレスのみが一致するエントリを検索するようにしてもよいし、送信元アドレスと送信先アドレスとプロトコルとが一致するエントリを検索するようにしてもよい。

【0027】精査部13は、上記のようにしてSPD12内のエントリを検索すると、そのエントリ内のインデックスを当該バケットに付加して振分部14に出力する（ステップST3）。ただし、そのエントリ内の処理指定が“暗号・認証”ではなく、“棄却”である場合には、そのバケットを出力せずに廃棄する。振分部14は、精査部13からインデックスが付加されたバケットを受けると、受信FIFO16aが空き状態の暗復号・認証処理部16を一つ選択し、その暗復号・認証処理部16に対して当該バケットを転送する（ステップST4）。なお、インデックスは、暗号アルゴリズムや暗号用鍵等と比べて、極めて少ない情報量であるため、バケットの通信路の帯域を圧迫するようなことはない。

【0028】暗復号・認証処理部16の制御部16bは、受信FIFO16aが振分部14から転送されたバケットを受信して格納すると、受信FIFO16aからバケットを取得し、図2に示すように、そのバケットに付加されているインデックスが指定するSAD15内の特定エントリから暗号アルゴリズムや暗号用鍵等を取得する（ステップST5）。

【0029】即ち、SAD15は、図2に示すように、暗号アルゴリズム、認証アルゴリズム、暗号用鍵及び認証用鍵等から構成された複数個のエントリを格納しているので、そのバケットに付加されているインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵

等を取得する。なお、SAD15は、通常、SRAMやDRAMなどのメモリにより実現される。

【0030】そして、暗復号・認証処理部16の制御部16bは、特定エントリから取得した暗号アルゴリズムが例えば暗号アルゴリズムAであれば、暗復号アルゴリズムA処理部16cを起動し、例えば暗号アルゴリズムBであれば、暗復号アルゴリズムB処理部16dを起動する。暗復号アルゴリズムA処理部16c又は暗復号アルゴリズムB処理部16dは、制御部16bから起動指令を受けると、制御部16bから出力された暗号用鍵を用いて暗号アルゴリズムA又は暗号アルゴリズムBを実行することにより、そのバケット内の暗号処理の対象ブロックを暗号化する（ステップST6）。

【0031】暗復号・認証処理部16の制御部16bは、暗復号アルゴリズムA処理部16c又は暗復号アルゴリズムB処理部16dの暗号化処理が完了すると、特定エントリから取得した認証アルゴリズムが例えば認証アルゴリズムAであれば、認証アルゴリズムA処理部16eを起動し、例えば認証アルゴリズムBであれば、認証アルゴリズムB処理部16fを起動する。認証アルゴリズムA処理部16e又は認証アルゴリズムB処理部16fは、制御部16bから起動指令を受けると、制御部16bから出力された認証用鍵を用いて認証アルゴリズムA又は認証アルゴリズムBを実行することにより、認証用のダイジェストを生成する（ステップST7）。

【0032】暗復号・認証処理部16の制御部16bは、認証アルゴリズムA処理部16e又は認証アルゴリズムB処理部16fが認証用のダイジェストを生成すると、暗復号アルゴリズムA処理部16c又は暗復号アルゴリズムB処理部16dにより暗号化されたバケットに当該ダイジェストを付加し、IPヘッダを生成してバケットのエンカプセル処理を行う（ステップST8）。そして、エンカプセル処理が完了すると、処理後のバケットを送信FIFO16gに格納する。

【0033】送信制御部17は、各暗復号・認証処理部16の送信FIFO16gから処理後のバケットを取り出して、処理後のバケットの順序を整列し、受信部11により受信されたバケットの順序に合わせるようにする（ステップST9）。送信部18は、送信制御部17から出力されたバケットにMACヘッダを付加して外部装置に送信する（ステップST10）。

【0034】次に暗号文データが格納されているバケットに対する認証処理を実施して、そのバケットを復号化する場合について説明する。受信部11が外部装置から暗号文データが格納されているバケットを受信すると、そのバケットのMACヘッダを削除して精査部13に出力する（ステップST11）。

【0035】精査部13は、受信部11からバケットを受けると、そのバケットからIPヘッダを取り出し、そのIPヘッダからバケットの送信元アドレス、送信先ア

ドレスやプロトコル等を取得する。そして、精査部13は、そのアドレスやプロトコルと一致するSPD12内のエントリを検索する（ステップST12）。

【0036】即ち、SPD12は、図2に示すように、送信元アドレス、送信先アドレス、プロトコル、送信先ポート番号、送信元ポート番号、SPI、処理指定（バケットに対する処理内容）、及びインデックス（SAD15内の特定エントリのアドレスを示すポインタ）から構成された複数のエントリを格納しているので、IPヘッダから取得したアドレスやプロトコルと一致する内容を有するエントリを検索する。ただし、必要に応じて送信先アドレスのみが一致するエントリを検索するようにしてもよいし、送信元アドレスと送信先アドレスとプロトコルとが一致するエントリを検索するようにしてもよい。

【0037】精査部13は、上記のようにしてSPD12内のエントリを検索すると、そのエントリ内のインデックスを当該バケットに付加して振分部14に出力する（ステップST13）。ただし、そのエントリ内の処理指定が“復号・認証”ではなく、“棄却”である場合には、そのバケットを出力せずに廃棄する。振分部14は、精査部13からインデックスが付加されたバケットを受けると、受信FIFO16aが空き状態の暗復号・認証処理部16を一つ選択して、その暗復号・認証処理部16に対して当該バケットを転送する（ステップST14）。なお、インデックスは、復号アルゴリズムや認証用鍵等と比べて、極めて少ない情報量であり、バケットの通信路の帯域を圧迫するようなことはない。

【0038】暗復号・認証処理部16の制御部16bは、受信FIFO16aが振分部14から転送されたバケットを受信して格納すると、受信FIFO16aからバケットを取得し、図2に示すように、そのバケットに付加されているインデックスが指定するSAD15内の特定エントリから復号アルゴリズムや認証用鍵等を取得する（ステップST15）。

【0039】即ち、SAD15は、図2に示すように、復号アルゴリズム、認証アルゴリズム、復号用鍵及び認証用鍵等から構成された複数のエントリを格納しているので、そのバケットに付加されているインデックスが指定する特定エントリから復号アルゴリズムや復号用鍵等を取得する。

【0040】そして、暗復号・認証処理部16の制御部16bは、特定エントリから取得した認証アルゴリズムが例えば認証アルゴリズムAであれば、認証アルゴリズムA処理部16eを起動し、例えば認証アルゴリズムBであれば、認証アルゴリズムB処理部16fを起動する。認証アルゴリズムA処理部16e又は認証アルゴリズムB処理部16fは、制御部16bから起動指令を受けると、制御部16bから出力された認証用鍵を用いて認証アルゴリズムA又は認証アルゴリズムBを実行する

ことにより、認証用のダイジェストを生成する（ステップST16）。

【0041】暗復号・認証処理部16の制御部16bは、認証アルゴリズムA処理部16e又は認証アルゴリズムB処理部16fが認証用のダイジェストを生成すると、そのダイジェストと、受信FIFO16aから取得したパケットに付加されているダイジェストとを比較する（ステップST17）。両者が一致する場合には、認証の成功を認定し、両者が一致しない場合には、認証の失敗を認定して、そのパケットを廃棄する（ステップST18）。

【0042】暗復号・認証処理部16の制御部16bは、上記のようにして認証の成功を認定すると、特定エントリから取得した復号アルゴリズムが例えば復号アルゴリズムAであれば、暗復号アルゴリズムA処理部16cを起動し、例えば復号アルゴリズムBであれば、暗復号アルゴリズムB処理部16dを起動する。暗復号アルゴリズムA処理部16c又は暗復号アルゴリズムB処理部16dは、制御部16bから起動指令を受けると、制御部16bから出力された復号用鍵を用いて復号アルゴリズムA又は復号アルゴリズムBを実行することにより、そのパケット内の復号処理の対象ブロックを復号化する（ステップST19）。

【0043】暗復号・認証処理部16の制御部16bは、暗復号アルゴリズムA処理部16c又は暗復号アルゴリズムB処理部16dの復号化処理が完了すると、復号化されたパケットからIPヘッダを削除して、パケットのデカプセル処理を行う。そして、デカプセル処理が完了すると、処理後のパケットを送信FIFO16gに格納する。

【0044】送信制御部17は、各暗復号・認証処理部16の送信FIFO16gから処理後のパケットを取り出して、処理後のパケットの順序を整列し、受信部11により受信されたパケットの順序に合わせるようにする（ステップST20）。送信部18は、送信制御部17から出力されたパケットにMACヘッダを付加して外部装置に送信する（ステップST21）。

【0045】以上で明らかなように、この実施の形態1によれば、インデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムや暗号用鍵等を取得して、そのパケットに対する暗号処理等を実行するように構成したので、パケット通信路の帯域圧迫を招くことなく、暗号処理や認証処理等を実行することができる結果、速やかに暗号処理や認証処理の実行を開始することができる効果を奏する。また、この実施の形態1によれば、各暗復号・認証処理部16毎に同一のSAD15を設けるように構成したので、並列化された各暗復号・認証処理部16は、他の暗復号・認証処理部16がSAD15にアクセスしているときも、そのアクセスの完了を待つことなく、SAD

D15にアクセスすることができる結果、速やかに暗号処理や認証処理の実行を開始することができる効果を奏する。

【0046】実施の形態2．図5はこの発明の実施の形態2によるパケット通信装置を示す構成図であり、図において、図1と同一符号は同一または相当部分を示すので説明を省略する。19はSAD15に格納されている情報を変更するための特定パケットを受信すると、その特定パケットに格納されているデータにしたがってSAD15を更新するSAD更新部（更新手段）である。

【0047】次に動作について説明する。上記実施の形態1では、SAD15に格納されているエントリ内の情報変更については特に言及していないが、SAD15に格納されているエントリ内の情報を変更するようにしてもよい。

【0048】即ち、受信部11がSAD15に格納されている情報を変更するための特定パケットを受信すると、振分部14が当該特定パケットをSAD更新部19に出力する。SAD更新部19は、振分部14から特定パケットを受けると、その特定パケットに格納されているデータにしたがってSAD15に格納されているエントリ内の情報を変更する。なお、SAD15に対するエントリの追加や削除を行うようにしてもよい。

【0049】実施の形態3．上記実施の形態2では、SAD更新部19が特定パケットに格納されているデータにしたがってSAD15に格納されているエントリ内の情報を変更するものについて示したが、図6に示すように、SAD更新部19の代わりに、一時保存バッファ20を設けることにより、SAD15を更新するようにしてもよい。

【0050】具体的には、受信部11がSAD15に格納されている情報を変更するための特定パケットを受信すると、精査部13が通常のパケットを有している場合、通常のパケットの処理を優先するため、振分部14が当該特定パケットを一時保存バッファ20に待避する。

【0051】振分部14は、精査部13において通常のパケットが無くなると、一時保存バッファ20に保存されている特定パケットを各暗復号・認証処理部16に転送する。各暗復号・認証処理部16の制御部16bは、精査部13から特定パケットを受けると、その特定パケットに格納されているデータにしたがってSAD15に格納されているエントリ内の情報を変更する。なお、SAD15に対するエントリの追加や削除を行うようにしてもよい。

【0052】

【発明の効果】以上のように、この発明によれば、インデックス付加手段によりインデックスが付加されたパケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、その

バケットに対する暗号処理を実行する処理実行手段を設けるように構成したので、速やかに暗号処理の実行を開始することができる効果がある。

【0053】この発明によれば、インデックス付加手段によりインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのバケットに対する復号処理を実行する処理実行手段を設けるように構成したので、速やかに復号処理の実行を開始することができる効果がある。

【0054】この発明によれば、インデックス付加手段によりインデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのバケットに対する認証処理を実行する処理実行手段を設けるように構成したので、速やかに認証処理の実行を開始することができる効果がある。

【0055】この発明によれば、複数の処理実行手段を設けて、インデックス付加手段が未処理中の処理実行手段に対してバケットを出力するように構成したので、処理の効率化を図ることができる効果がある。

【0056】この発明によれば、各処理実行手段毎に同一のデータベースを設けるように構成したので、ある処理実行手段がデータベースにアクセスしているときも、そのアクセスの完了を待つことなく、その他の処理実行手段がデータベースにアクセスすることができる結果、速やかに暗号処理等の実行を開始することができる効果がある。

【0057】この発明によれば、データベースに格納されている情報を変更するための特定バケットを受信すると、その特定バケットに格納されているデータにしたがってデータベースを更新する更新手段を設けるように構成したので、通常のバケットに対する処理に影響を与えることなく、データベースを更新することができる効果がある。

【0058】この発明によれば、インデックス付加手段がデータベースに格納されている情報を変更するための特定バケットを受信すると、その特定バケットをバッファに一時的に保存し、処理実行手段が未処理のバケットが存在しないとき特定バケットを取得し、その特定バケットに格納されているデータにしたがってデータベースを更新するように構成したので、通常のバケットに対する処理に影響を与えることなく、データベースを更新することができる効果がある。

【0059】この発明によれば、インデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから暗号アルゴリズムと暗号用鍵を取得して、そのバケットに対する暗号処理を実行するように構成したので、速やかに暗号処理の実行を開始することができる効果がある。

【0060】この発明によれば、インデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから復号アルゴリズムと復号用鍵を取得して、そのバケットに対する復号処理を実行するように構成したので、速やかに復号処理の実行を開始することができる効果がある。

【0061】この発明によれば、インデックスが付加されたバケットを受けると、そのインデックスが指定する特定エントリから認証アルゴリズムと認証用鍵を取得して、そのバケットに対する認証処理を実行するように構成したので、速やかに認証処理の実行を開始することができる効果がある。

【図面の簡単な説明】

【図1】 この発明の実施の形態1によるバケット通信装置を示す構成図である。

【図2】 SPD及びSADの格納内容を示す説明図である。

【図3】 この発明の実施の形態1によるバケット通信方法を示すフローチャートである。

【図4】 この発明の実施の形態1によるバケット通信方法を示すフローチャートである。

【図5】 この発明の実施の形態2によるバケット通信装置を示す構成図である。

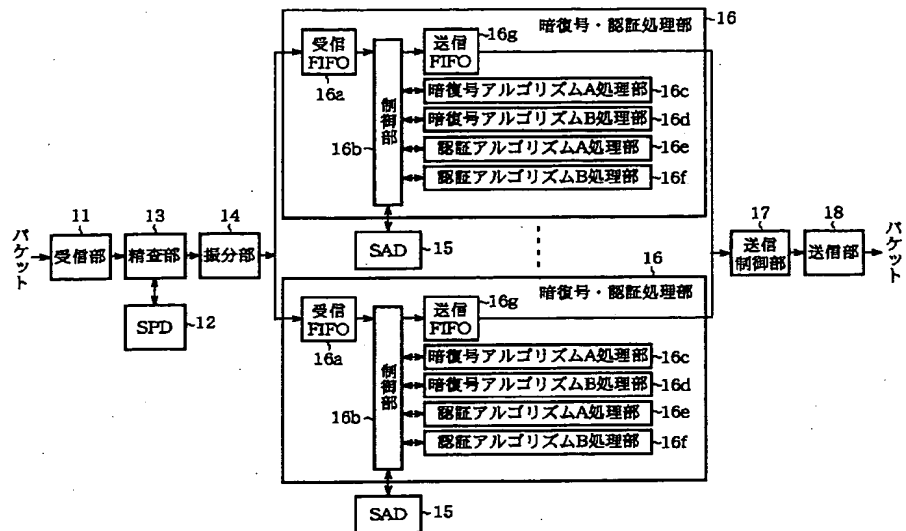
【図6】 この発明の実施の形態3によるバケット通信装置を示す構成図である。

【図7】 従来のバケット通信装置を示す構成図である。

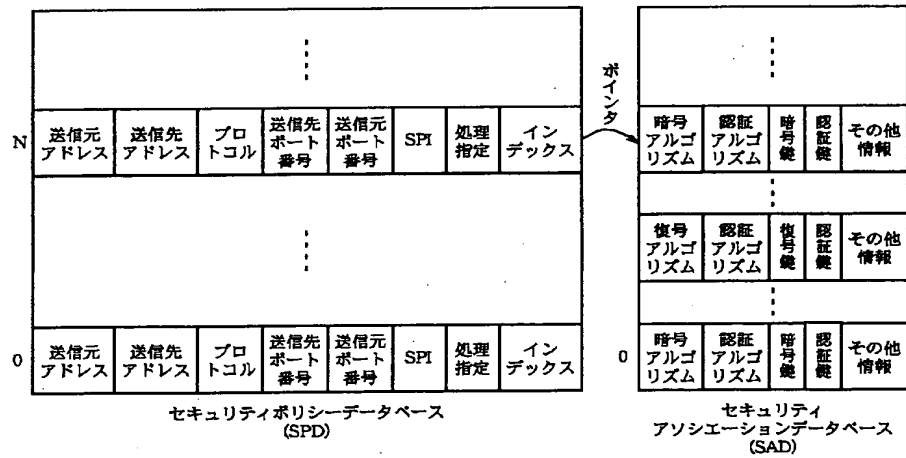
【符号の説明】

11 受信部（インデックス付加手段）、12 SPD（インデックス付加手段）、13 精査部（インデックス付加手段）、14 振分部（インデックス付加手段）、15 SAD（データベース）、16 暗復号・認証処理部（処理実行手段）、16a 受信FIFO、16b 制御部、16c 暗復号アルゴリズムA処理部、16d 暗復号アルゴリズムB処理部、16e 認証アルゴリズムA処理部、16f 認証アルゴリズムB処理部、16g 送信FIFO、17 送信制御部、18 送信部。

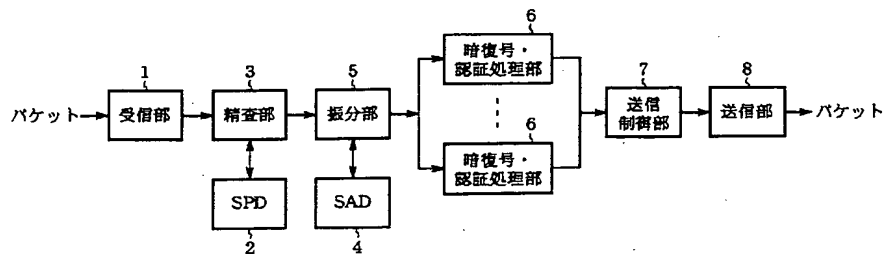
【図1】



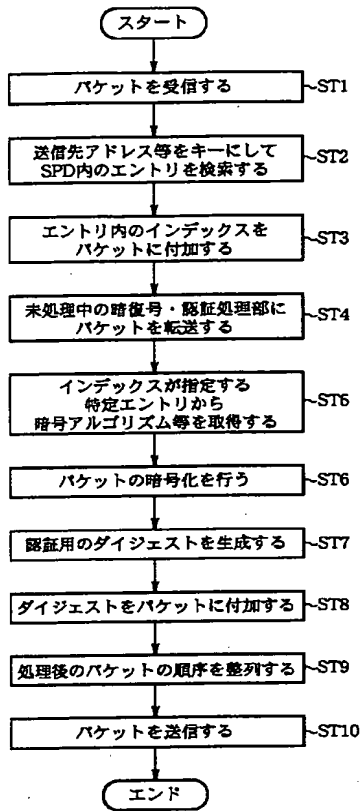
【図2】



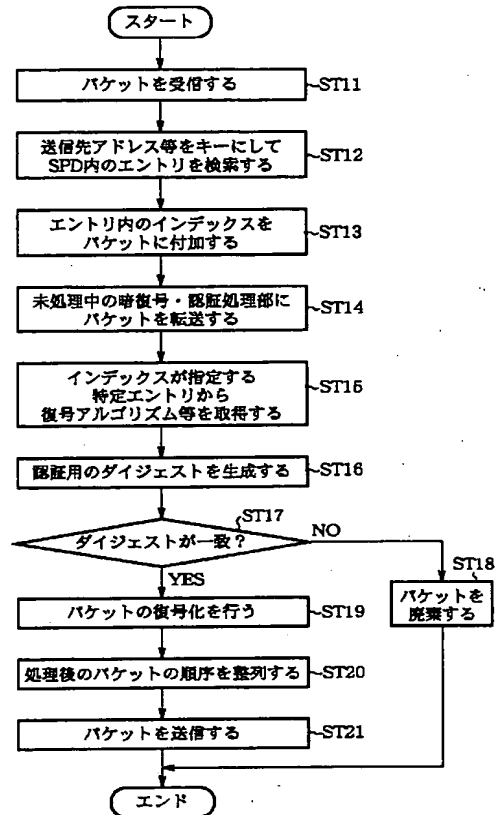
【図7】



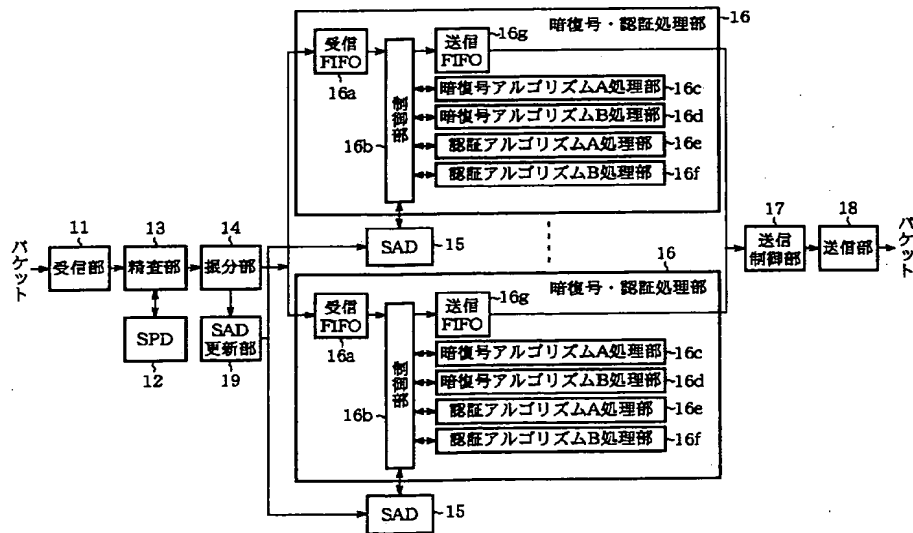
【図3】



【図4】



【図5】



【図6】

